CLAIMS

1.   A method for rights management of digital content and secure delivery of digital content documents from a publisher site to an unsecure site, the method comprising:

    (a)   encrypting each digital content document at the publisher site with a key to generate encrypted document content;

    (b)   computing for each document, from the encrypted document content for that document, a document identifier that cannot be derived solely from the encrypted version of the requested document;

    (c)   creating a list of document identifier and decryption key pairs;

    (d)   assembling the encrypted document content for each content document and the list into a distribution archive;

    (e)   encrypting the distribution archive with a scheduled key;

    (f)   installing a content server at the unsecure site; and

    (g)   sending the distribution archive from the publisher site to the content server.

2.   The method of claim 1 wherein step (a) comprises compressing each document before encrypting the document.

3.   The method of claim 1 wherein step (b) comprises computing a document identifier from the encrypted document content and a text string at the publisher site.

4.   The method of claim 1 further comprising:

    (h)   at the unsecure site, decrypting the distribution archive with the scheduled key, extracting the encrypted document content and storing the encrypted document content in a storage located at the unsecure site.

30

5. The method of claim 4 wherein a user at the unsecure location accesses the content server from a browser and wherein the method further comprises:

(i)   downloading a secure viewer program into the browser;

(j)   using the viewer program to request a document from the content server;

(k)   downloading an encrypted version of the requested document from the content server to the viewer; and

(l)   using the viewer to calculate a document identifier from the encrypted version of the requested document and to send the document identifier to the content server.

6. The method of claim 5 further comprising:

(m)   using the document identifier in the content server to retrieve a decryption key from the list and downloading the decryption key to the viewer program; and

(n)   using the downloaded key in the viewer program to decrypt the encrypted version of the document and present the document to the user.

7. The method of claim 1 further comprising:

(h)   monitoring content access at the unsecure site; and

(i)   creating a log file at the unsecure site from the monitored activities.

8. The method of claim 7 further comprising:

(j)   sending the log file to the publisher site in return for a distribution archive containing new content.

9. The method of claim 8 further comprising:

(k)   extracting the contents of the log file at the publisher site;

(l)   formatting the extracted contents and providing a report from the formatted contents to a reporting client.

31

1   10.   The method of claim 7 wherein step (h) comprises monitoring user activities

2   including login to the system, registration, creation of a user profile and the

3   reading and printing of selected content documents.

1   11.   Apparatus for rights management of digital content and secure delivery of digital

2   content documents from a publisher site to an unsecure site, the apparatus

3   comprising:

4   means for encrypting each digital content document at the publisher site

5   with a key to generate encrypted document content;

6   an OID calculator that computes for each document, from the encrypted

7   document content for that document, a document identifier that cannot be

8   derived solely from the encrypted version of the requested document;

9   means for creating a list of document identifier and decryption key pairs;

10   means for assembling the encrypted document content for each content

11   document and the list into a distribution archive;

12   an encryptor that encrypts the distribution archive with a scheduled key;

13   means for installing a content server at the unsecure site; and

14   means for sending the distribution archive from the publisher site to the

15   content server.

1   12.   The apparatus of claim 11 wherein the means for encrypting each digital content

2   document comprises a compressor that compresses each document and an

3   encryption engine that encrypts the compressed document.

1   13.   The apparatus of claim 11 wherein the OID calculator comprises means for

2   computing a document identifier from the encrypted document content and a text

3   string at the publisher site.

1   14.   The apparatus of claim 11 further comprising a decryption engine located at the
2   unsecure site that decrypts the distribution archive with the scheduled key, a file
3   decompressor that extracts the encrypted document content and stores the
4   encrypted document content in a storage located at the unsecure site.

1   15.   The apparatus of claim 14 wherein a user at the unsecure location accesses the
2   content server from a browser and wherein the apparatus further comprises
3   means for downloading a secure viewer program into the browser, means for
4   using the viewer program to request a document from the content server; means
5   for downloading an encrypted version of the requested document from the
6   content server to the viewer; an OID calculator in the viewer that calculates a
7   document identifier from the encrypted version of the requested document and
8   means for sending the document identifier to the content server.

1   16.   The apparatus of claim 15 further comprising means for using the document
2   identifier in the content server to retrieve a decryption key from the list, means for
3   downloading the decryption key to the viewer program and means for using the
4   downloaded key in the viewer program to decrypt the encrypted version of the
5   document and present the document to the user.

1   17.   The apparatus of claim 11 further comprising a log server that monitors content
2   access at the unsecure site and means for creating a log file at the unsecure site
3   from the monitored activities.

1   18.   The apparatus of claim 17 further comprising means for sending the log file to the
2   publisher site in return for a distribution archive containing new content.

1   19.   The apparatus of claim 18 further comprising a reporting server that extracts the
2   contents of the log file at the publisher site, formats the extracted contents and
3   provides a report from the formatted contents to a reporting client.

1 20. The apparatus of claim 17 wherein the log server comprises means for

2   monitoring user activities including login to the system, registration, creation of a

3   user profile and the reading and printing of selected content documents.

1 21. A computer program product for rights management of digital content and secure

2   delivery of digital content documents from a publisher site to an unsecure site,

3   the computer program product comprising a computer usable medium having

4   computer readable program code thereon, including:

5   program code for encrypting each digital content document at the

6   publisher site with a key to generate encrypted document content;

7   program code for computing for each document, from the encrypted

8   document content for that document, a document identifier that cannot be

9   derived solely from the encrypted version of the requested document;

10   program code for creating a list of document identifier and decryption key

11   pairs;

12   program code for assembling the encrypted document content for each

13   content document and the list into a distribution archive;

14   program code for encrypting the distribution archive with a scheduled key;

15   program code for installing a content server at the unsecure site; and

16   program code for sending the distribution archive from the publisher site to

17   the content server.

1 22. The computer program product of claim 21 wherein the program code for

2   encrypting each digital content document at the publisher site comprises program

3   code for compressing each document before encrypting the document.

1 23. The computer program product of claim 21 wherein the program code for

2   computing a document identifier comprises program code for computing a

3 document identifier from the encrypted document content and a text string at the

4 publisher site.

1 24. The computer program product of claim 21 further comprising program code at

2 the unsecure site, for decrypting the distribution archive with the scheduled key,

3 extracting the encrypted document content and storing the encrypted document

4 content in a storage located at the unsecure site.

1 25. The computer program product of claim 24 wherein a user at the unsecure

2 location accesses the content server from a browser and wherein the computer

3 program product further comprises:

4   program code for downloading a secure viewer program into the browser;

5   program code in the viewer program for requesting a document from the

6 content server;

7   program code for downloading an encrypted version of the requested

8 document from the content server to the viewer; and

9   program code in the viewer for calculating a document identifier from the

10 encrypted version of the requested document and for sending the document

11 identifier to the content server.

1 26. The computer program product of claim 25 further comprising:

2   program code for using the document identifier in the content server to

3 retrieve a decryption key from the list and downloading the decryption key to the

4 viewer program; and

5   program code for using the downloaded key in the viewer program to

6 decrypt the encrypted version of the document and present the document to the

7 user.

1 27. The computer program product of claim 21 further comprising:

2   program code for monitoring content access at the unsecure site; and

3   program code for creating a log file at the unsecure site from the

4   monitored activities.

1   28.   The computer program product of claim 27 further comprising:

2   program code for sending the log file to the publisher site in return for a

3   distribution archive containing new content.

1   29.   The computer program product of claim 28 further comprising:

2   program code for extracting the contents of the log file at the publisher

3   site;

4   program code for formatting the extracted contents and providing a report

5   from the formatted contents to a reporting client.

1   30.   The computer program product of claim 27 wherein the program code for

2   monitoring content access comprises program code for monitoring user activities

3   including login to the system, registration, creation of a user profile and the

4   reading and printing of selected content documents.